PASSAIC PUBLIC SCHOOLS
Passaic, New Jersey

Policy

FILE CODE: 3520
____ Mandated
____ Monitored
_X_ Other Reasons

CYBERSECURITY AWARENESS TRAINING POLICY

PURPOSE

This policy aims to establish a framework for the education and training of faculty, staff, and students to improve understanding and mitigate risks to data and privacy while using technology and digital resources provided by Passaic Public Schools. Mandatory training is to be conducted by the Division of Information Technology (IT) annually to provide updated cybersecurity awareness and ensure compliance with applicable Federal and New Jersey state laws, regulations, and guidelines related to the protection of student data and privacy.

POLICY

This policy is applicable to all departments and users of information technology resources and assets.

1. CYBERSECURITY AWARENESS TRAINING

All employees and contractors with access to student data and/or digital resources are required to complete a mandatory annual cybersecurity awareness training program. The training program shall cover, but not be limited to:

a. Cybersecurity Threats and Protective Measures: Identification and prevention of common cybersecurity threats, such as phishing, social engineering, ransomware, and malware, as well as best practices for maintaining secure systems, networks, and devices. Understanding data sensitivity levels and methods for handling, storage, and transmission of sensitive data.
b. Password Management and Secure Browsing: Guidelines for creating and managing strong, unique passwords, and recommendations for secure browsing.
c. Risk factor: Understanding the risk posed to organizations from cybercrime related data loss.

2. INCIDENT REPORTING

All employees, contractors, and students are responsible for reporting any security incidents, breaches, or violations of this policy to the school district's Director of the Division of Information Technology.

3. PRACTICAL EXERCISES

Division of Information Technology will perform practical exercises in security training that reinforce training objectives; practical exercises may include:

a. Simulated phishing emails that are designed to mimic real-world phishing attempts. These emails may include various tactics, such as spoofed sender addresses, urgent requests, or links to fake websites.
b. A review of training completion and failure rates will be conducted to determine the need for supplemental training, which will be informed by the frequency of user failures to practical exercises.

4. POLICY REVIEW AND UPDATE

In addition to providing security awareness training to staff, the Division of Information Technology will review and update training annually, so the training curriculum stays current on new and emerging threats. Assessment results will be analyzed to identify areas where the security awareness training program can be improved. Feedback from employees shall be solicited to ensure that the training programs are relevant, engaging, and effective in promoting security awareness and responsible digital behavior.

5. Consequences

Failure to adhere to the security awareness training policy may result in disciplinary action, which can encompass various consequences in combination, such as the following:

1. Warning
2. Loss of privilege to access the Internet
3. Loss of computer privileges in the Passaic Public Schools
4. Referral to administration for discipline

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Director of the Division of Information Technology. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken, initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein. The Director shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT

Division of Information Technology (IT) – Conducts practical exercises to assess the efficacy of training, manages incident reporting and response, oversees training procedures, validates training, and maintains training materials.

REFERENCES

New Jersey Student Digital Privacy and Parental Rights Act (N.J.S.A. 18A:36-39)
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
Children's Internet Protection Act (CIPA) (47 U.S.C. § 254)
Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501–6506)
Cybersecurity Information Sharing Act of 2015 (CISA) (6 U.S.C. §§ 1501-1510)

Passaic Public School Policies

Internet Use Policy - File Code 6142.10
Internet Safety and Technology Use Policy - File Code 6142.10
Acceptable Use Agreement – File Code 6142.10

First Reading:	September 26, 2023
Second Reading:	October 30, 2023
Approved:	October 30, 2023